AXBOROTNI RUXSATSIZ FOYDALANISHDAN HIMOYALASH: HUQUQIY, TASHKILIY VA TEXNIK YONDASHUVLAR.

Bobojonov Ilg'or Axmadtullo o'g'li
Toshkent viloyati
Piskent tumani 1-son politexnikumi
Informatika va axborot texnologiyalari fani o'qituvchisi

Annotatsiya: Axborot xavfsizligini ta’minlash zamonaviy raqamli dunyoda eng muhim masalalardan biridir. Axborot va kommunikatsiya texnologiyalari (AKT) ob’ektlarida axborot xavfsizligini ko’plab xavf-xatarlardan himoya qilish maqsadida maxsus usullar va vositalar to’plami qo’llaniladi. Ushbu maqola axborotni himoya qilishning huquqiy, tashkiliy va texnik usullarini tahlil qiladi, ularning har biri bir nechta xavflarni bartaraf etishga xizmat qiladi. Huquqiy usullar axborot xavfsizligi tizimlarini rasmiy ravishda joriy etish va boshqarish uchun asos bo’lib xizmat qilsa, tashkiliy usullar xodimlar va infratuzilma xavfsizligini ta’minlaydi, texnik usullar esa zamonaviy apparat va dasturiy vositalar orqali axborotni himoya qiladi. Maqolada O’zbekiston Respublikasining axborot xavfsizligi sohasidagi qonunchilik asoslari, shuningdek, global tendensiyalar va zamonaviy yondashuvlar ham ko’rib chiqiladi.

Kalit so’zlar: axborot xavfsizligi, kompyuter jinoyatchiligi, huquqiy himoya, tashkiliy choralar, texnik vositalar, kriptografiya, biometrik autentifikatsiya, kiberxavfsizlik, maxfiy ma’lumotlar, davlat sirlari.

Kirish

Zamonaviy dunyoda axborot eng muhim resurslardan biriga aylandi. Axborot va kommunikatsiya texnologiyalarining jadal rivojlanishi, internet va raqamli tarmoqlarning kengayishi axborotni ruxsatsiz foydalanish, o’g’irlash yoki buzib

tashlash xavfini oshirdi. Shu sababli, axborot xavfsizligini ta’minlash har qanday tashkilot, davlat yoki shaxs uchun strategik ahamiyatga ega. Ushbu maqola axborotni himoya qilishning huquqiy, tashkiliy va texnik usullarini tahlil qiladi, shuningdek, O’zbekiston Respublikasining ushbu sohadagi qonunchilik tajribasi va zamonaviy kiberxavfsizlik yondashuvlarini ko’rib chiqadi.

Axborot xavfsizligini ta’minlashning huquqiy asoslari

Axborot xavfsizligini huquqiy himoya qilish axborotni qonuniy boshqarish va xavf-xatarlarni bartaraf etish uchun asosiy vosita hisoblanadi. O’zbekiston Respublikasida axborot xavfsizligi sohasidagi qonunchilik “Axborot, axborotlashtirish va axborotni himoya qilish to’g’risida”gi qonun (2019-yil 11-sentabr, O’RQ-572-son) asosida tashkil etilgan. Ushbu qonun axborot resurslarini ochiq va cheklangan murojaat toifalariga ajratish, maxfiy ma’lumotlarni himoya qilish va kompyuter jinoyatchiligiga qarshi choralar ko’rishni tartibga soladi.

Huquqiy himoya qilishning asosiy yo’nalishlari quyidagilardan iborat:

1. **Kompyuter jinoyatchiligiga qarshi choralar**: O’zbekiston Respublikasi Jinoyat kodeksining 278-1, 278-2 va 278-3-moddalari kompyuter axborotiga noqonuniy murojaat qilish, zararli dasturlarni yaratish va tarqatish, shuningdek, axborot tizimlari ishini buzish kabi jinoyatlarni aniqlaydi va ularga jazo choralarini belgilaydi.
2. **Mualliflik huquqlarini himoya qilish**: Dasturiy ta’minot va intellektual mulkni himoya qilish uchun maxsus qonunlar qabul qilingan bo’lib, ular dasturchilar va axborot tizimlari ishlab chiquvchilarining huquqlarini kafolatlaydi.
3. **Xalqaro hamkorlik**: O’zbekiston xalqaro kiberxavfsizlik shartnomalariga qo’shilish orqali global axborot xavfsizligi standartlariga rioya qiladi, masalan, Budapest konvensiyasi (Kiberjinoyatchilikka qarshi konvensiya) tamoyillariga moslashish.

4. **Davlat sirlari va maxfiy ma’lumotlarni himoya qilish**: “Davlat sirlari to’g’risida”gi qonun (2018-yil, O’RQ-493-son) davlat sirlarini himoya qilish tartibini belgilaydi, maxfiy ma’lumotlarni esa tashkilotlar va shaxslar tomonidan qo’llaniladigan maxsus choralar orqali himoya qilinadi.

Huquqiy himoya tizimi shaxsiy ma’lumotlarning maxfiyligini ta’minlash, shaxsiy va oilaviy sirlarni, shuningdek, tijorat va xizmat sirlarini qonuniy himoya qilishni kafolatlaydi. Masalan, shaxsiy ma’lumotlarni himoya qilish bo’yicha qonun loyihasi (2023-yilda takomillashtirilgan) fuqarolarni shaxsiy ma’lumotlarining noqonuniy ishlatilishidan himoya qilishga xizmat qiladi.

Tashkiliy himoya choralari

Tashkiliy choralar axborot xavfsizligini ta’minlashda muhim ahamiyatga ega bo’lib, tashkilot ichidagi jarayonlar va xodimlar faoliyatini tartibga soladi. Ushbu choralar quyidagi yo’nalishlarni qamrab oladi:

1. **Xodimlarni tanlab olish va o’qitish**: Xodimlarning malakasini oshirish, axborot xavfsizligi bo’yicha maxsus treninglar o’tkazish va ularga maxfiy ma’lumotlar bilan ishlash qoidalarini o’rgatish.
2. **Fizik xavfsizlik**: Kompyuter markazlari va server xonalarini himoya qilish, masalan, biometrik autentifikatsiya tizimlari (barmoq izi, yuzni aniqlash) va videokuzatuv tizimlaridan foydalanish.
3. **Tizimning ishlash qobiliyatini tiklash**: Favqulodda holatlarda (masalan, kiberhujumlar yoki apparat nosozliklari) axborot tizimlarini tiklash rejasini ishlab chiqish va sinovdan o’tkazish.
4. **Javobgarlikni belgilash**: Axborot xavfsizligi bo’yicha mas’ul shaxslarni tayinlash va ularning faoliyatini monitoring qilish.
5. **Axborot resurslarini joylashtirish**: Serverlar va axborot tizimlarini xavfsiz joylarda joylashtirish, masalan, maxsus himoyalangan ma’lumotlar markazlarida.

Tashkiliy choralar ichida “bir kishi printsipi”ni cheklash muhim ahamiyatga ega, ya’ni muhim vazifalarni faqat bitta shaxs tomonidan bajarilishiga yo’l qo’ymaslik. Bu xodimlarning xatolarini yoki qasddan zarar yetkazishini oldini olishga yordam beradi.

Texnik himoya usullari

Texnik himoya usullari axborot xavfsizligini ta’minlashda eng ilg’or va dinamik rivojlanayotgan sohadir. Ular apparatli, dasturiy va apparat-dasturiy vositalarga bo’linadi. Zamonaviy texnologiyalar asosida quyidagi yo’nalishlar muhim hisoblanadi:

1. **Ruxsatsiz kirishdan himoya**: Kirishni boshqarish tizimlari (Access Control Systems) va kirish matrisalari yordamida axborot resurslariga ruxsatsiz murojaat qilishning oldini olish. Masalan, ro’lga asoslangan kirishni boshqarish (RBAC) va majburiy kirishni boshqarish (MAC) tizimlari keng qo’llaniladi.
2. **Virusga qarshi himoya**: Zamonaviy antivirus dasturlari, masalan, Kaspersky, Norton yoki ESET, zararli dasturlarni aniqlash va bartaraf etishda samarali hisoblanadi. Shuningdek, sun’iy intellektga asoslangan xavfsizlik tizimlari kiberxavflarni real vaqt rejimida aniqlaydi.
3. **Kriptografik himoya**: Axborotni shifrlash uchun AES-256, RSA va kvant kriptografiyasi kabi usullar qo’llaniladi. Bu maxfiy ma’lumotlarning uzatilishi va saqlanishini xavfsiz qiladi.
4. **Tarmoq xavfsizligi**: Brandmauerlar (firewalls), tarmoq trafikini tahlil qiluvchi IDS/IPS tizimlari va VPN texnologiyalari tarmoq hujumlaridan himoya qiladi.
5. **Elektromagnit va akustik himoya**: Maxfiy ma’lumotlarning elektromagnit nurlanishlar orqali o’g’irlanishini oldini olish uchun maxsus ekranlashtirilgan jihozlar va xonalar (Faraday qafasi) ishlatiladi.

Zamonaviy tendensiyalar orasida sun’iy intellekt va mashinaviy o’qitishga asoslangan xavfsizlik tizimlari, shuningdek, blokcheyn texnologiyalari keng

qo’llanilmoqda. Masalan, blokcheyn axborotning o’zgarmasligini ta’minlashda muhim vosita sifatida ishlatiladi.

O’zbekistonda axborot xavfsizligining hozirgi holati

O’zbekistonda axborot xavfsizligi sohasidagi qonunchilik bazasi so’nggi yillarda sezilarli darajada rivojlandi. “Axborot, axborotlashtirish va axborotni himoya qilish to’g’risida”gi qonun va “Davlat sirlari to’g’risida”gi qonun axborot resurslarini tasniflash, maxfiy ma’lumotlarni himoya qilish va kiberjinoyatchilikka qarshi kurashishni tartibga soladi. Shu bilan birga, O’zbekiston Respublikasi Prezidentining “Axborot-kommunikatsiya texnologiyalarini rivojlantirish bo’yicha chora-tadbirlar to’g’risida”gi farmonlari (masalan, 2020-yil PF-6079-son) kiberxavfsizlik infratuzilmasini rivojlantirishga xizmat qiladi.

Ammo, global tendensiyalarga moslashishda bir qator muammolar mavjud:

- **Malakali kadrlar yetishmasligi**: Kiberxavfsizlik bo’yicha mutaxassislarning yetishmasligi tashkilotlar uchun katta xavf tug’diradi.
- **Texnologik infratuzilma**: Zamonaviy xavfsizlik vositalarini joriy etishda moliyaviy va texnik cheklovlar mavjud.
- **Xalqaro hamkorlik**: Global kiberxavfsizlik standartlariga to’liq moslashish uchun qo’shimcha choralar talab etiladi.

Zamonaviy yondashuvlar va kelajakdagi imkoniyatlar

Axborot xavfsizligi sohasidagi zamonaviy yondashuvlar sun’iy intellekt, mashinaviy o’qitish va blokcheyn texnologiyalariga asoslanadi. Masalan, SIEM (Security Information and Event Management) tizimlari real vaqt rejimida xavf-xatarlarni aniqlash va ularga javob berish imkonini beradi. Kvant hisoblash texnologiyalari esa kelajakda shifrlash usullarini tubdan o’zgartirishi kutilmoqda.

O’zbekistonda axborot xavfsizligini rivojlantirish uchun quyidagi chora-tadbirlarni amalga oshirish zarur:

1. **Ta’lim va kadrlar tayyorlash**: Kiberxavfsizlik bo’yicha maxsus ta’lim dasturlarini kengaytirish va xalqaro sertifikatlarga ega mutaxassislar tayyorlash.
2. **Texnologik yangilanish**: Zamonaviy xavfsizlik vositalarini, masalan, sun’iy intellektga asoslangan tizimlarni joriy etish.
3. **Xalqaro hamkorlikni kengaytirish**: Xalqaro tashkilotlar bilan hamkorlikni mustahkamlash va global kiberxavfsizlik tashabbuslarida ishtirok etish.

Xulosa

Axborot xavfsizligini ta’minlash zamonaviy dunyoda strategik ahamiyatga ega. Huquqiy, tashkiliy va texnik usullar birgalikda axborot resurslarini ruxsatsiz foydalanishdan himoya qilishga xizmat qiladi. O’zbekiston Respublikasi qonunchilik bazasi va infratuzilmasi ushbu sohada sezilarli yutuqlarga erishgan bo’lsa-da, zamonaviy kiberxavflarga qarshi kurashda global standartlarga moslashish va yangi texnologiyalarni joriy etish zarur. Ushbu maqola axborot xavfsizligining muhim jihatlarini yoritib, kelajakdagi rivojlanish yo’nalishlarini belgilab beradi.

Foydalanilgan adabiyotlar:

1. O’zbekiston Respublikasining “Axborot, axborotlashtirish va axborotni himoya qilish to’g’risida”gi qonuni, 2019-yil, O’RQ-572-son.
2. O’zbekiston Respublikasining “Davlat sirlari to’g’risida”gi qonuni, 2018-yil, O’RQ-493-son.
3. G’ulomov, S.S. (2009). *Informatika va axborot texnologiyalari*. Toshkent: Iqtisodiyot.
4. Aripov, M., Begalov, B., & boshq. (2009). *Axborot texnologiyalari*. Toshkent: Noshir.
5. Makarova, N.V. (2005). *Informatika*. Toshkent: Talqin.

6. O’zbekiston Respublikasi Prezidentining “Axborot-kommunikatsiya texnologiyalarini rivojlantirish bo’yicha chora-tadbirlar to’g’risida”gi farmoni, 2020-yil, PF-6079-son.
7. https://www.gov.uz – O’zbekiston Respublikasi hukumati portali.